

Amendments to the Claims:

The claims below replace all prior versions and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A secure computer device, comprising:
means for locally-authenticating a user of the device;
means for granting previously authorized ~~non-controlling~~ access to the device if the user is locally authenticated;
means for generating a remote authentication request after a successful local authentication of the user; ~~and~~
means for granting access to new activities and control parameters on the computer device if remote authentication is successful; and
means for allowing continued work on authorized activity; and
means for denying access to new activities until the authorized activity is completed.

2. (original) The device recited in claim 1 further comprising means for authorizing the user in response to the successful local authentication.

3. (original) The device recited in claim 2 further comprising means for withdrawing the authorization in response to a reply from the server.

4. (original) The device recited in claim 1 further comprising means for updating the local user authenticating means in response to a reply from the server.

5. (original) The device recited in claim 2 further comprising means for updating the local user authenticating means in response to a reply from the server.

6. (original) The device recited in claim 3 further comprising means for updating the local user authenticating means in response to the reply from the server.

7. (currently amended) A computer security method, comprising the steps of:
 locally-authenticating a user of a client device;
 granting previously authorized ~~non-controlling~~ access to the device if the user is locally authenticated;
 generating an authentication request to a server after a successful local authentication of the user; and
 granting access to new activities and control parameters on the computer device if remote authentication is successful unless the authorized activity is not completed, wherein the new activity is denied; and
 storing identification data from a subsequent user while a previous user's activity is being completed.

8. (original) The method recited in claim 7, further comprising the step of authorizing the user in response to a successful local authentication.

9. (original) The method recited in claim 8 further comprising the step of withdrawing the authorization in response to a reply from the server.

10. (original) The method recited in claim 7 further comprising the step of updating user authentication data stored on the client in response to a reply from the server.

11. (original) The method recited in claim 8 further comprising the step of updating user authentication data stored on the client in response to the reply from the server.

12. (original) The method recited in claim 9 further comprising the step of updating user authentication data stored on the client in response to a reply from the server.

13. (currently amended) A computer readable medium, comprising:
logic for locally-authenticating a user of a client device;
logic configured to grant previously authorized ~~non-controlling~~ access to the device if the user is locally authenticated;
logic for generating an authentication request to a server after a successful local authentication; and
logic configured to grant access to new activities and control parameters on the computer device if remote authentication is successful unless the authorized activity is not completed, wherein the new activity is denied; and
storing identification data from a subsequent user while a previous user's activity is being completed.

14. (original) The computer readable medium recited in claim 13, further comprising logic for authorizing the user in response to the successful local authentication.

15. (original) The computer readable medium recited in claim 14, further comprising logic for withdrawing an authorization in response to a reply from the server.

16. (original) The computer readable medium recited in claim 13, further comprising logic for updating user authentication data stored on the client in response to a reply from the server.

17. (original) The computer readable medium recited in claim 14, further comprising logic for updating user authentication data stored on the client in response to a reply from the server.

18. (original) The computer readable medium recited in claim 15, further comprising logic for updating user authentication data stored on the client in response to a reply from the server.

19. (currently amended) A secure computer system, comprising:

- a client having a client database for locally-authenticating a user;
- an authentication device that grants previously authorized non-controlling access if the user is locally authenticated;
- a server, in communication with the client, having a server database for remotely-authenticating the user in response to a request from the client after a successful local authentication;
- wherein the authentication device grants access to new activities and control parameters on the computer device if remote authentication is successful unless the authorized activity is not completed, wherein the new activity is denied;
- storing identification data from a subsequent user while a previous user's activity is being completed;
- means for updating the client database according to results of the local and remote authentications; and
- means for limiting a number of times that a particular client database and/or record in any, or all, of the client databases will be updated during any period of time and/or total number of updates.

20. (original) The secure computer system recited in claim 19, further comprising

- means for authorizing a user in response to a successful local authentication; and
- means for withdrawing the authorization in response to an unsuccessful remote authentication.